

What is claimed is:

1. An information processing device comprising:
 - a data input interface for inputting encrypted data;
 - 5 a decryption module for decrypting encrypted data inputted by the data input interface using a decryption key forming a pair with a first encryption key used to encrypt the data;
 - an encryption module for encrypting data decrypted by the decryption module using a second encryption key different from the
 - 10 first encryption key; and
 - a storage device for storing data encrypted by the encryption module.
2. The information processing device of claim 1, wherein
- 15 an expiration date is not set for the second encryption key.
3. The information processing device of claim 1, wherein
 - the data input interface also inputs unencrypted data, and
 - the encryption module also encrypts unencrypted data input
 - 20 by the data input interface.
4. The information processing device of claim 1, further comprising:
 - a key generator for generating the second encryption key.
- 25 5. The information processing device of claim 4, further comprising:
 - volatile memory; and
 - a memory controller for storing the second encryption key in the volatile memory.

6. The information processing device of claim 4, wherein
the key generator generates the second encryption key using
information characteristic to the device itself.

5 7. The information processing device of claim 4, wherein
the key generator generates the second encryption key when
power to the device is turned on.

8. The information processing device of claim 4, further comprising:
10 a media reader capable of being installed with a removable
portable storage media storing key generation parameters for reading
a key generation parameter stored on the installed portable storage
media, wherein
the key generator generates the second encryption key using
15 the key generation parameter.

9. The information processing device of claim 4, further comprising:
a security level setting module for setting a security level
for the information processing device, wherein
20 the key generator generates the second encryption key of a
key length corresponding to the security level set at the security
level setting module.

10. The information processing device of claim 4, further comprising:
25 a region setting module for receiving settings for a region
where the device is to be used, wherein
the key generator generates the second encryption key of a
key length corresponding to the region set at the region setting
module.

11. The information processing device of claim 1, further comprising:

a media reader capable of being installed with a removable portable storage media storing the encryption key, wherein

5 the encryption module reads the second encryption key from the portable storage media installed in the media reader and performs encryption.

12. The information processing device of claim 1, equipped with
10 a plurality of the storage devices, and having second encryption keys corresponding to each storage device, wherein the encryption module performs encryption using the second encryption key corresponding to storage device decided by a data storage destination.

15

13. The information processing device of claim 1, having encryption keys corresponding to each user using the device, wherein

the encryption module performs encryption using an encryption key for the user corresponding to the data.

20

14. The information processing device of claim 1, further comprising:

deciding means for deciding whether or not to encrypt data inputted by the data input interface, wherein

25 the encryption module encrypts data decided upon for encryption by the deciding means.

15. The information processing device of claim 14, wherein

the deciding means decides to encrypt when data inputted by the data input interface is encrypted.

16. The information processing device of claim 1, further comprising a printer for decrypting and printing data stored in the storage device.

5

17. A method for storing data inputted to an information processing device, comprising the steps of:

inputting encrypted data;

decrypting encrypted data inputted using a decryption key

10 forming a pair with a first encryption key used to encrypt the data;

encrypting decrypted data using a second encryption key different from the first encryption key; and

storing data encrypted using the second encryption key.

15 18. The information processing device of claim 17, further comprising a step of:

storing the second encryption key in the volatile memory.

20